ABSTRACT

The invention is designed to eliminate or minimize the liability associated with "packet flooding" attacks originating from within a local area network connected to an external network such as one controlled by a university or governmental organization. In these attacks, an attacker uses up all available bandwidth to a victim with useless data. The invention performs its function by identifying and classifying data packets arriving at a “Reverse Firewall” for transmission to the external network using various techniques. For example, data packets that are sent in response to data packets received from the external network will receive a different classification and thus allocation of resources than data packets not sent in response to previously received packets. The invention also serves to maximize use of data packet handling resources within the local area network by identifying those data packets that are requests for service, measuring the amount of service required by those packets, storing and recalling past service measurements and thus determining an appropriate allocation of resources.